Refine Search

Search Results -

Terms	Documents
L32 and ("key size")	1

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search: L33

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Friday, September 02, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L33	L32 and ("key size")	1	L33
L32	L31 and (L11 or L12 or L21)	8	L32
L31	L30 and (request with access)	100	L31
L30	L5 and authoriz$6	101	L30
L29	L28 and L6	0	L29
L28	L27 and (user near (identif$4 or key$1 or label$1))	17	L28
L27	L26 and L2	34	L27
L26	(L13 or L14 or L15 or L16 or L17 or L18) and L1	440	L26
L25	L24 and ("key size")	1	L25
L24	L23 and (user near identif$4)	3	L24
L23	L22 and L6	8	L23
L22	(L11 or L12 or L21) and l4	136	L22
L21	713/$.ccls.	26691	L21
L20	715/$.ccls.	22416	L20

L19	715/743.ccls.	28	L19
L18	715/741.ccls.	128	L18
L17	713/200.ccls.	3133	L17
L16	709/229.ccls.	2494	L16
L15	709/225.ccls.	1918	L15
L14	709/219.ccls.	3210	L14
L13	709/217.ccls.	3418	L13
L12	709/$.ccls.	38572	L12
L11	707/$.ccls.	28930	L11
L10	L9 and (user near identif$4)	2	L10
L9	L8 and match$3	5	L9
L8	L1 and L6	8	L8
L7	L6 and L5	1	L7
L6	generat$3 with (security near context)	35	L6
L5	L4 and L3	109	L5
L4	L1 and L2	281	L4
L3	(logon or (log near on)) same (user near identif$4)	405	L3
L2	context with security	2767	L2
L1	(logon or (log near on)) same user	3790	L1

END OF SEARCH HISTORY

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 1 of 1 returned.

☐ 1. Document ID: US 20020184217 A1

Using default format because multiple data bases are involved.

L33: Entry 1 of 1 File: PGPB Dec 5, 2002

PGPUB-DOCUMENT-NUMBER: 20020184217
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020184217 A1

TITLE: Systems and methods for state-less authentication

PUBLICATION-DATE: December 5, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Bisbee, Stephen F.	Baltimore	MD	US	
Moskowitz, Jack J.	Ellicon City	MD	US	
Becker, Keith F.	Baltimore	MD	US	
Peterson, Ellis K.	Arnold	MD	US	
Twaddell, Gordon W.	Milleraville	MD	US	

US-CL-CURRENT: 707/9

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L32 and ("key size")	1

Display Format: - Change Format

Previous Page Next Page Go to Doc#

Refine Search

Search Results -

Terms	Documents
L6 and L5	1

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L7

Refine Search

Recall Text Clear Interrupt

Search History

DATE: Friday, September 02, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L7	L6 and L5	1	L7
L6	generat$3 with (security near context)	35	L6
L5	L4 and L3	109	L5
L4	L1 and L2	281	L4
L3	(logon or (log near on)) same (user near identif$4)	405	L3
L2	context with security	2767	L2
L1	(logon or (log near on)) same user	3790	L1

END OF SEARCH HISTORY

First Hit Previous Doc Next Doc Go to Doc#

End of Result Set

Generate Collection Print

L7: Entry 1 of 1 File: PGPB Dec 5, 2002

PGPUB-DOCUMENT-NUMBER: 20020184217
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020184217 A1

TITLE: Systems and methods for state-less authentication

PUBLICATION-DATE: December 5, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Bisbee, Stephen F.	Baltimore	MD	US	
Moskowitz, Jack J.	Ellicon City	MD	US	
Becker, Keith F.	Baltimore	MD	US	
Peterson, Ellis K.	Arnold	MD	US	
Twaddell, Gordon W.	Milleraville	MD	US	

APPL-NO: 09/ 839551 [PALM]
DATE FILED: April 19, 2001

INT-CL: [07] G06 F 7/00

US-CL-PUBLISHED: 707/9
US-CL-CURRENT: 707/9

REPRESENTATIVE-FIGURES: 2

ABSTRACT:

Systems and methods for providing user logon and state-less authentication are described in a distributed processing environment. Upon an attempted access by a user to an online resource, transaction, or record, a logon component asks the user to supply a logon ID and a password. The logon component verifies the provided information, and upon successful identification, a security context is constructed from information relevant to the user. The security context is sent to the user and is presented to the system each time the user attempts to invoke a new resource, such as a program object, transaction, record, or certified printer avoiding the need for repeated logon processing.

Previous Doc Next Doc Go to Doc#

Hit List

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Search Results - Record(s) 1 through 1 of 1 returned.

☐ 1. Document ID: US 20020184217 A1

Using default format because multiple data bases are involved.

L7: Entry 1 of 1 File: PGPB Dec 5, 2002

PGPUB-DOCUMENT-NUMBER: 20020184217
PGPUB-FILING-TYPE: new
DOCUMENT-IDENTIFIER: US 20020184217 A1

TITLE: Systems and methods for state-less authentication

PUBLICATION-DATE: December 5, 2002

INVENTOR-INFORMATION:

NAME	CITY	STATE	COUNTRY	RULE-47
Bisbee, Stephen F.	Baltimore	MD	US	
Moskowitz, Jack J.	Ellicon City	MD	US	
Becker, Keith F.	Baltimore	MD	US	
Peterson, Ellis K.	Arnold	MD	US	
Twaddell, Gordon W.	Milleraville	MD	US	

US-CL-CURRENT: 707/9

Full | Title | Citation | Front | Review | Classification | Date | Reference | Sequences | Attachments | Claims | KWIC | Draw D

Clear | Generate Collection | Print | Fwd Refs | Bkwd Refs | Generate OACS

Terms	Documents
L6 and L5	1

Display Format: - Change Format

Previous Page Next Page Go to Doc#

Refine Search

Search Results -

Terms	Documents
L24 and ("key size")	1

Database: US Pre-Grant Publication Full-Text Database; US Patents Full-Text Database; US OCR Full-Text Database; EPO Abstracts Database; JPO Abstracts Database; Derwent World Patents Index; IBM Technical Disclosure Bulletins

Search: L25

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Friday, September 02, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L25	L24 and ("key size")	1	L25
L24	L23 and (user near identif$4)	3	L24
L23	L22 and L6	8	L23
L22	(L11 or L12 or L21) and l4	136	L22
L21	713/$.ccls.	26691	L21
L20	715/$.ccls.	22416	L20
L19	715/743.ccls.	28	L19
L18	715/741.ccls.	128	L18
L17	713/200.ccls.	3133	L17
L16	709/229.ccls.	2494	L16
L15	709/225.ccls.	1918	L15
L14	709/219.ccls.	3210	L14
L13	709/217.ccls.	3418	L13
L12	709/$.ccls.	38572	L12

L11	707/$.ccls.	28930	L11
L10	L9 and (user near identif$4)	2	L10
L9	L8 and match$3	5	L9
L8	L1 and L6	8	L8
L7	L6 and L5	1	L7
L6	generat$3 with (security near context)	35	L6
L5	L4 and L3	109	L5
L4	L1 and L2	281	L4
L3	(logon or (log near on)) same (user near identif$4)	405	L3
L2	context with security	2767	L2
L1	(logon or (log near on)) same user	3790	L1

END OF SEARCH HISTORY

Refine Search

Search Results -

Terms	Documents
L28 and L6	0

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L29

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Friday, September 02, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=OR			
L29	L28 and L6	0	L29
L28	L27 and (user near (identif$4 or key$1 or label$1))	17	L28
L27	L26 and L2	34	L27
L26	(L13 or L14 or L15 or L16 or L17 or L18) and L1	440	L26
L25	L24 and ("key size")	1	L25
L24	L23 and (user near identif$4)	3	L24
L23	L22 and L6	8	L23
L22	(L11 or L12 or L21) and l4	136	L22
L21	713/$.ccls.	26691	L21
L20	715/$.ccls.	22416	L20
L19	715/743.ccls.	28	L19
L18	715/741.ccls.	128	L18
L17	713/200.ccls.	3133	L17
L16	709/229.ccls.	2494	L16

L15	709/225.ccls.	1918	L15
L14	709/219.ccls.	3210	L14
L13	709/217.ccls.	3418	L13
L12	709/$.ccls.	38572	L12
L11	707/$.ccls.	28930	L11
L10	L9 and (user near identif$4)	2	L10
L9	L8 and match$3	5	L9
L8	L1 and L6	8	L8
L7	L6 and L5	1	L7
L6	generat$3 with (security near context)	35	L6
L5	L4 and L3	109	L5
L4	L1 and L2	281	L4
L3	(logon or (log near on)) same (user near identif$4)	405	L3
L2	context with security	2767	L2
L1	(logon or (log near on)) same user	3790	L1

END OF SEARCH HISTORY

127
9-2-05

e-mail

Results for "(((security <near> context) <and> (access <near> resource) <and> (request &l..."

Your search matched 2 of 1229994 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

(((security <near> context) <and> (access <near> resource) <and> (request <near> a

Check to search only within this results set

» Key

Display Format: Citation Citation & Abstract

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select Article Information

1. **Distributing Internet services to the network's edge**
Weaver, A.C.; Condry, M.W.;
Industrial Electronics, IEEE Transactions on
Volume 50, Issue 3, June 2003 Page(s):404 - 411
Digital Object Identifier 10.1109/TIE.2003.812278
AbstractPlus | References | Full Text: PDF(599 KB) IEEE JNL

2. **Security policies to mitigate insider threat in the document control domain**
Suranjan Pramanik; Vidyaraman Sankaranarayanan; Shambhu Upadhyaya;
Computer Security Applications Conference, 2004. 20th Annual
6-10 Dec. 2004 Page(s):304 - 313
Digital Object Identifier 10.1109/CSAC.2004.35
AbstractPlus | Full Text: PDF(216 KB) IEEE CNF

Results for "(((generat* <near> security <near> context) <and> (access <near> resource))&..."
Your search matched 1 of 1229994 documents.
A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

(((generat* <near> security <near> context) <and> (access <near> resource))<in>me

Check to search only within this results set

» Key

Display Format: Citation Citation & Abstract

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

1. **Routing with confidence: supporting discretionary routing requirements in policy based net**
Apu Kapadia; Prasad Naldurg; Campbell, R.H.;
Policies for Distributed Systems and Networks, 2004. POLICY 2004. Proceedings. Fifth IEEE Inten
7-9 June 2004 Page(s):45 - 54
Digital Object Identifier 10.1109/POLICY.2004.1309149
AbstractPlus | Full Text: PDF(353 KB) IEEE CNF

Results for "(((security <near> context) <and> (access <near> resource) <and> (key <ne..."

Your search matched 0 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

» Search Options

View Session History

New Search

Modify Search

(((security <near> context) <and> (access <near> resource) <and> (key <near> size)) >>

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistance revising your search

1246
9-7-05

Terms used **generating security context access resource security context id key size**

Found **1** of **160,906**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 1 of 1

Relevance scale

1 Authentication services for computer networks and electronic messaging systems

Keok Auyong, Chye-Lin Chee

July 1997 **ACM SIGOPS Operating Systems Review**, Volume 31 Issue 3

Full text available: pdf(1.03 MB) Additional Information: full citation, abstract, index terms

The paper surveys the authentication services used by modern computer systems and presents the major operational authentication services employed by commercial companies, banking as well as government departments. As distributed system services are susceptible to a variety of threats mounted by intruders as well as legitimate users of the system, password-based authentication is not suitable for use on computer networks.

Results 1 - 1 of 1

Terms used **generating security context access resource security context id key size user logon**

Found **3** of **160,906**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 3 of 3

Relevance scale

1 Regaining single sign-on taming the beast

Divyangi Anchan, Mahmoud Pegah

September 2003 **Proceedings of the 31st annual ACM SIGUCCS conference on User services**

Full text available: pdf(217.34 KB) Additional Information: full citation, abstract, references, index terms

It has been our effort at Ringling school to provide our campus community with the capability to uniformly access resources across multiple platforms. Empowering the user with a single sign-on capability has multifold benefits. It greatly improves user experience and relieves the user from the burden of remembering multiple user-id and password pairs. On the administrative side, help desk costs are noticeably reduced and security improved, as users are not tempted to 'store' multiple passwords i ...

Keywords: LDAP, RPC, account synchronization, active directory (AD), active directory service interfaces (ADSI), password synchronization, single sign-on

2 Authentication services for computer networks and electronic messaging systems

Keok Auyong, Chye-Lin Chee

July 1997 **ACM SIGOPS Operating Systems Review**, Volume 31 Issue 3

Full text available: pdf(1.03 MB) Additional Information: full citation, abstract, index terms

The paper surveys the authentication services used by modern computer systems and presents the major operational authentication services employed by commercial companies, banking as well as government departments. As distributed system services are susceptible to a variety of threats mounted by intruders as well as legitimate users of the system, password-based authentication is not suitable for use on computer networks.

3 A distributed system security architecture: applying the transport layer security protocol

Mohammad Mirhakkak

October 1993 **ACM SIGCOMM Computer Communication Review**, Volume 23 Issue 5

Full text available: pdf(892.06 KB) Additional Information: full citation, abstract, index terms

A great deal of attention has been given to the development of Open Systems Interconnection (OSI) security protocols in recent years. However, limited work has been dedicated to using these protocols to develop security architectures for securing distributed systems consisting of trusted computer systems communicating via untrusted networks. This

paper presents an overview of the Transport Layer Security Protocol (TLSP) and discusses its application to the development of a security architecture ...

Results 1 - 3 of 3

```
Set     Items   Description
S1      54663   AUTHENTICAT? OR LOGIN OR LOGON OR SIGNIN OR SIGNON OR (LOG
             OR SIGN)()("IN" OR ON) OR PASSWORD? OR PASS()(WORD OR WORDS OR
              PHRASE?)
S2     160041   GLOBAL UNIVERSAL OR "NOT"()STATEFUL OR STATELESS OR REUSE?
              OR RECYCLE? OR USE()AGAIN? OR RE()(USE OR CYCLE OR USING) OR
             REUSING OR RECYCLING OR STATE()LESS OR SESSIONLESS
S3     409552   KEY OR KEYS OR IDENTIFIER? OR BIT()STRING? ? OR ID OR IDS -
             OR LABEL OR LABELS
S4    2216079   SECURITY()CONTEXT? OR ORGANIZATION? OR USER? OR INDIVIDUAL?
              OR MEMBER? OR EMPLOYEE?
S5    5755856   LOCATION? OR ROLE? OR ACCESS()LEVEL? OR EXPIRATION? OR POS-
             ITION? OR TIME OR DATE OR TIMES OR DATES OR DURATION
S6         54   S1 AND S2 AND S3
S7         38   S6 AND (S4 OR S5)
S8         25   S7 NOT AD=20010419:20030419
S9         21   S8 NOT AD=20030419:20050905
S10        17   S9 AND IC=(G06F OR H04L)
S11        30   S6 AND (KEY OR KEYHANDLE? OR KEYS)
S12        13   S11 NOT S8
S13        26   S1 AND S2 AND S4 AND S5
S14        22   S13 AND IC=(G06F OR H04L OR H04N)
S15        34   S12 OR S14
S16        21   S15 NOT S7
S17        11   S16 NOT AD=20010419:20040419
S18        11   S17 NOT AD=20040419:20050922
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200555
        (c) 2005  Thomson Derwent
```

18/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

06506329 **Image available**
REMOTE **AUTHENTICATION** SYSTEM

PUB. NO.: 2000-092046 [JP 2000092046 A]
PUBLISHED: March 31, 2000 (20000331)
INVENTOR(s): NAKAMURA HIROSHI
BABA YOSHIMASA
SADAKANE TETSUO
FUJII TERUKO
APPLICANT(s): MITSUBISHI ELECTRIC CORP
APPL. NO.: 10-257813 [JP 98257813]
FILED: September 11, 1998 (19980911)
INTL CLASS: **H04L-009/32** ; **G06F-015/00** ; G06T-007/00; **H04L-009/14**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a remote **authentication** system and a remote **authentication** method which are highly reliable in security, and can surely **authenticate** an indivisual by means of biometrics information being the **individual** information of a **user** while protecting the biometrics information.
SOLUTION: Since the biometrics information being the **individual** information of the **user** is ciphered and the biometrics information is transferred on a network 2 in a state decipherable only by an **authentication** server 3 specified by the **user** , the privacy of the **user** which is the biometrics information is surely protected in the form of reflecting the intention of the **user** . Also, since the **date** and **time** of preparing **authentication** information are confirmed in the **authentication** server 3, the illegal **reuse** of the **authentication** information is prevented. Further, since whether or not the **authentication** is performed by the **authentication** server 3 is confirmed on an **authentication** request side, thus this system is maintained high in security.

18/5/8 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014758948 **Image available**
WPI Acc No: 2002-579652/200262
XRPX Acc No: N02-459982
Authentication **device by biometric data, separates** time **-stamp data that is added to biometric data based on which** authentication **of** user **is performed**
Patent Assignee: TAKAMI S (TAKA-I)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 2002169781	A	20020614	JP 2000367053	A	20001201	200262	B

Priority Applications (No Type Date): JP 2000367053 A 20001201
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 2002169781	A		4	G06F-015/00	

Abstract (Basic): JP 2002169781 A
NOVELTY - The device destroys a portion of the biometric data based on the **time** -stamp data. The **time** -stamp data added to the biometric data is separated and the **authentication** of a **user** is performed. After **authentication** , the biometric data is stored in a database (30) along with the **time** -stamp data portion based on a predetermined priority.
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for **authentication** method by biometric data.
USE - For **authentication** of **user** using biometric data.
ADVANTAGE - The biometric data with **time** -stamp data cannot be utilized for another **time** , hence the **recycling** of the biometric data is prevented, and ensures greater safety and effectiveness.
DESCRIPTION OF DRAWING(S) - The figure shows the outline structure of the **authentication** device by biometric data. (Drawing includes non-English language text).
Database (30)
pp; 4 DwgNo 1/1
Title Terms: AUTHENTICITY; DEVICE; DATA; SEPARATE; **TIME** ; STAMP; DATA; ADD ; DATA; BASED; AUTHENTICITY; **USER** ; PERFORMANCE
Derwent Class: S05; T01
International Patent Class (Main): **G06F-015/00**
International Patent Class (Additional): G06K-017/00; G06T-007/00
File Segment: EPI

```
Set     Items   Description
S1      54663   AUTHENTICAT? OR LOGIN OR LOGON OR SIGNIN OR SIGNON OR (LOG
             OR SIGN)()("IN" OR ON) OR PASSWORD? OR PASS()(WORD OR WORDS OR
              PHRASE?)
S2     160041   GLOBAL UNIVERSAL OR "NOT"()STATEFUL OR STATELESS OR REUSE?
              OR RECYCLE? OR USE()AGAIN? OR RE()(USE OR CYCLE OR USING) OR
             REUSING OR RECYCLING OR STATE()LESS OR SESSIONLESS
S3     409552   KEY OR KEYS OR IDENTIFIER? OR BIT()STRING? ? OR ID OR IDS -
             OR LABEL OR LABELS
S4    2216079   SECURITY()CONTEXT? OR ORGANIZATION? OR USER? OR INDIVIDUAL?
              OR MEMBER? OR EMPLOYEE?
S5    5755856   LOCATION? OR ROLE? OR ACCESS()LEVEL? OR EXPIRATION? OR POS-
             ITION? OR TIME OR DATE OR TIMES OR DATES OR DURATION
S6         54   S1 AND S2 AND S3
S7         38   S6 AND (S4 OR S5)
S8         25   S7 NOT AD=20010419:20030419
S9         21   S8 NOT AD=20030419:20050905
S10        17   S9 AND IC=(G06F OR H04L)
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200555
         (c) 2005  Thomson Derwent
```

10/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

06807096 **Image available**
COMMON-USE COMPUTER USING METHOD

PUB. NO.: 2001-034580 [JP 2001034580 A]
PUBLISHED: February 09, 2001 (20010209)
INVENTOR(s): NAKAHAMA KIYOSHI
SAITO RYUICHI
APPLICANT(s): NIPPON TELEGR & TELEPH CORP (NTT)
APPL. NO.: 11-206026 [JP 99206026]
FILED: July 21, 1999 (19990721)
INTL CLASS: **G06F-015/00** ; **G06F-001/00** ; **H04L-009/08** ; **H04L-009/32**

ABSTRACT

PROBLEM TO BE SOLVED: To actualize a common-use computer using method which can maintain high security without making a **user** pay attention to environment that the **user** has constructed and a file that the **user** has generated by immediately constructing the environment of a personal computer which was used once by another personal computer.

SOLUTION: On a common-use computer system device , the **user** after being **authenticated** for use performs a operation process wanted to be tried (F3), an information group that the **user** stored in a storage means of a personal computer C11 by decentralization in the operation process or at a **time** at the end according to the operation process is ciphered in the personal computer C11 with a **key** corresponding to the **user** , and the obtained ciphered sentence is stored in a storage means of a server S1 as ciphered difference information as it is. An information group which is deleted from the storage means of the personal computer C11 according to the operation process is deleted from the storage means of the server S1 (F4) and **reused** when the common-use computer system device is used next **time** (F6).

10/5/7 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014845166 **Image available**
WPI Acc No: 2002-665872/200271
Related WPI Acc No: 2002-636098; 2002-665871; 2003-046403; 2003-057728; 2003-090715
XRPX Acc No: N02-526825
Internet-based authentication **system for medical application,** authenticates user **identification information using** authentication **service identified by service** identifier
Patent Assignee: HEIL J A (HEIL-I); ROYER B L (ROYE-I)
Inventor: HEIL J A; ROYER B L
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020095605	A1	20020718	US 2001261148	P	20010112	200271 B
			US 2001817324	A	20010326	

Priority Applications (No Type Date): US 2001261148 P 20010112; US 2001817324 A 20010326
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020095605	A1		20	H04L-009/32	Provisional application US 2001261148

Abstract (Basic): US 20020095605 A1

NOVELTY - An **authentication** processor receives a **user** identification information including a **user identifier** . A communication processor communicates an **authentication** service **identifier** and the **user identifier** to a managing application which **authenticates** the **user** using the **authentication** service identified by the service **identifier** .

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for **authentication** method.

USE - For **authenticating** physicians and other **individuals** for on-line access of medical records.

ADVANTAGE - Provides common and essential session properties for providing access to an array of comprehensive information sources and related services. Facilitates **reuse** and interoperability of web-based application in multiple sequences and current operation configurations.

DESCRIPTION OF DRAWING(S) - The figure illustrates command interaction between concurrently-operating applications, a web browser, and a manager.

pp; 20 DwgNo 4/16

Title Terms: BASED; AUTHENTICITY; SYSTEM; MEDICAL; APPLY; **USER** ; IDENTIFY; INFORMATION; AUTHENTICITY; SERVICE; IDENTIFY; SERVICE; IDENTIFY
Derwent Class: S05; T01
International Patent Class (Main): **H04L-009/32**
File Segment: EPI

10/5/9 (Item 3 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014026199 **Image available**
WPI Acc No: 2001-510413/200156
Method for managing lottery for recycling **publicity booklet and increasing effect of publicity**
Patent Assignee: PARK Y K (PARK-I)
Inventor: PARK Y K
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
KR 2001008278	A	20010205	KR 200069120	A	20001120	200156	B

Priority Applications (No Type Date): KR 200069120 A 20001120
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
KR 2001008278	A		1	G06F-017/6004	

Abstract (Basic): KR 2001008278 A
NOVELTY - A method for managing a lottery for **recycling** a publicity booklet and increasing the effect of publicity is provided to allocate a unique number to the publicity booklet, to use the unique number as a number for receiving a gift on an online network, and to select some of the unique numbers voted by **members** .
DETAILED DESCRIPTION - If a **user** accesses a server via an online network, the **user** is **authenticated** (1-1). The unique number is allocated to a service **user** . The unique number that the **user** receives can be the unique number of the publicity booklet distributed via an offline system or the **ID** of the **user** . If the **user** inputs his/her unique number into a unique number giving engine(1-3),(1-2), the engine(1-3) assigns the unique number to the **user** . The **user** accesses the server to check the gift number. The weight of the unique number can be increased, based on the right of the **user** . The unique number which participates in the event of the lottery the most frequently is determined as a winning number of the gift.
pp; 1 DwgNo 1/10
Title Terms: METHOD; MANAGE; LOTS; **RECYCLE** ; PUBLICITY; BOOK; INCREASE; EFFECT; PUBLICITY
Derwent Class: T05
International Patent Class (Main): **G06F-017/6004**
File Segment: EPI

10/5/13 (Item 7 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013065234 **Image available**
WPI Acc No: 2000-237106/200020
XRPX Acc No: N00-177829
Concurrent or multiple user **access controller for on-line computer systems, includes binary bits which are indicative of current logins in same word**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: ZHAO Y
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 6035404	A	20000307	US 97926207	A	19970909	200020	B

Priority Applications (No Type Date): US 97926207 A 19970909
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 6035404	A		11	G06F-017/40	

Abstract (Basic): US 6035404 A
NOVELTY - Internal **user ID** is assigned to each **user** . A **user login** map (ULM) for recording current number of logins, contains binary words each with several binary bits. One or more binary bits in same word are indicative of current logins. A record of each access session are temporarily kept in progress where one bit of word indicates current status for single **user ID** .
DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for method of controlling **user** access over **stateless** network.
USE - For control of **user** access for **stateless** network.
ADVANTAGE - A state look-up table is used to manage the distribution of account between all authorized **users** , such that equitable use of limited facility can be had by all **users** , when more than the permitted number of **users** try to access the system at same **time** .
DESCRIPTION OF DRAWING(S) - The figure shows flow chart for control of access to **users** .
pp; 11 DwgNo 7/9
Title Terms: CONCURRENT; MULTIPLE; **USER** ; ACCESS; CONTROL; LINE; COMPUTER; SYSTEM; BINARY; BIT; INDICATE; CURRENT; WORD
Derwent Class: T01; T05
International Patent Class (Main): **G06F-017/40**
File Segment: EPI

10/5/14 (Item 8 from file: 350)
DIALOG(R)File 350:Derwent WPIX

012578904 **Image available**
WPI Acc No: 1999-385011/199932
XRPX Acc No: N99-288364
Access enabling method of web documents stored in secure distributed file system e.g. world wide web
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: AULT M B; BURNETT R C; PLASSMANN E R; RICH B A; ROSILES M A; SHI S; SHRADER T J L
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5918228	A	19990629	US 97790042	A	19970128	199932	B

Priority Applications (No Type Date): US 97790042 A 19970128
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5918228	A		10	G06F-017/00	

Abstract (Basic): US 5918228 A
NOVELTY - If the web transaction request received from web client (10) is determined to be originated from **authenticated user** of distributed file system, the web server **reuses** the **authentication identifier** of **user** credential to retrieve file from distributed file system on behalf of web client.
DETAILED DESCRIPTION - The web server is temporarily inhibited from using the **authentication identifier** upon logging of web transaction, until next web transaction is performed by the **user** .
INDEPENDENT CLAIMS are also included for the following:
(a) computer program product;
(b) computer connected in distributed computing environment
USE - For enabling web server to impersonate **user** of distributed file system to obtain secure access to supported web documents in world wide web environment.
ADVANTAGE - Extends functionality of existing standalone web servers in enterprise environment to improve scalability, file availability and security features of distributed file systems. The **user** with an off-the-shelf browser is enabled to easily access the web information stored in distributed file system name space without any additional software on client machine.
DESCRIPTION OF DRAWING(S) - The figure shows process flow diagram illustrating web transaction.
Web client (10)
pp; 10 DwgNo 3/6
Title Terms: ACCESS; ENABLE; METHOD; WEB; DOCUMENT; STORAGE; SECURE; DISTRIBUTE; FILE; SYSTEM; WORLD; WIDE; WEB
Derwent Class: T01
International Patent Class (Main): **G06F-017/00**
File Segment: EPI

10/5/15 (Item 9 from file: 350)
DIALOG(R)File 350:Derwent WPIX

011799900 **Image available**
WPI Acc No: 1998-216810/199819
XRPX Acc No: N98-171432

Preventing unauthorised access in secure computer system in e.g. bank - recording chaotic random source to form binary string to which hash function is applied to obtain seed to be inserted into random number generator

Patent Assignee: SILICON GRAPHICS INC (SILI-N)
Inventor: MENDE R G; NOLL L C; SISODIYA S
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5732138	A	19980324	US 96592891	A	19960129	199819	B

Priority Applications (No Type Date): US 96592891 A 19960129
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5732138	A		16	H04L-009/22	

Abstract (Basic): US 5732138 A

The unauthorised access prevention involves the generation of pseudo-random numbers, where initially the state of a chaotic system is digitised, by recording (100) a chaotic source e.g. a lava lamp, to form (105) a binary string. A cryptographic hash function i.e. NIST SHS-1 is applied (110) to the binary string to produce a second binary string.

The second binary string is used (115) to seed a random number generator (120) of Blum-Blum-Shub type, the output of which is used in forming a **password** or cryptographic **key** for use in a security system. Further **passwords** or **keys** can be generated by passing (125,130) the seed through the number generator again.

USE - For encryption of bank transactions and accounts.

ADVANTAGE - Enables generation of long sequence of pseudo-random numbers with reasonable computation **time** , by generating shorter random numbers and **reusing** the seed generated from them, thus avoiding **time** bottlenecks in computation caused by repeated random number generation.

Dwg.1/7

Title Terms: PREVENT; UNAUTHORISED; ACCESS; SECURE; COMPUTER; SYSTEM; BANK; RECORD; RANDOM; SOURCE; FORM; BINARY; STRING; HASH; FUNCTION; APPLY; OBTAIN; SEED; INSERT; RANDOM; NUMBER; GENERATOR
Derwent Class: T01; T05; W01
International Patent Class (Main): **H04L-009/22**
File Segment: EPI

```
Set     Items   Description
S1      48006   AUTHENTICAT? OR LOGIN OR LOGON OR SIGNIN OR SIGNON OR (LOG
             OR SIGN)()("IN" OR ON) OR PASSWORD? OR PASS()(WORD OR WORDS OR
              PHRASE?)
S2     288248   GLOBAL UNIVERSAL OR "NOT"()STATEFUL OR STATELESS OR REUSE?
              OR RECYCLE? OR USE()AGAIN? OR RE()(USE OR CYCLE OR USING) OR
             REUSING OR RECYCLING OR STATE()LESS OR SESSIONLESS
S3    1009407   KEY OR KEYS OR IDENTIFIER? OR BIT()STRING? ? OR ID OR IDS -
             OR LABEL OR LABELS
S4    4402447   SECURITY()CONTEXT? OR ORGANIZATION? OR USER? OR INDIVIDUAL?
              OR MEMBER? OR EMPLOYEE?
S5   11569016   LOCATION? OR ROLE? OR ACCESS()LEVEL? OR EXPIRATION? OR POS-
            ITION? OR TIME OR DATE OR TIMES OR DATES OR DURATION
S6         99   S1 AND S2 AND S3
S7         58   S6 AND (S4 OR S5)
S8         95   S6 AND (KEY OR KEYHANDLE? OR KEYS)
S9         38   S1 AND S2 AND S4 AND S5
S10      2395   (ONE OR SINGLE OR ONLY OR CENTRAL? OR UNIVERSAL? OR GLOBAL?
              OR SYSTEM()WIDE)(2N)S1
S11    731850   (MULTIPL? OR PLURAL OR MANY OR SEVERAL OR DIFFERENT OR VAR-
             IOUS OR VARIET? OR DISTRIBUTED)(2N)(SYSTEM? OR MODULE? OR PRO-
             GRAM? OR NODE? ? OR WORKSTATION? OR WORK()STATION?)
S12       193   S10 AND S11
S13        67   S12 AND (KEY OR KEYHANDLE? OR KEYS OR KEYPAIR?)
S14        19   S12 AND (ALGORITHM? OR FORMULA? OR CALCULATION?)
S15        99   S9 OR S14 OR S7
S16        77   RD (unique items)
S17        39   S16 NOT PY>2001
S18         1   S13 AND S8
File   8:Ei Compendex(R) 1970-2005/Aug W3
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Aug
         (c) 2005 ProQuest Info&Learning
File  56:Computer and Information Systems Abstracts 1966-2005/Aug
         (c) 2005 CSA.
File  57:Electronics & Communications Abstracts 1966-2005/Aug
         (c) 2005 CSA.
File  65:Inside Conferences 1993-2005/Aug W4
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Aug W3
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Jul W1
         (c)2005 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Sep 01
         (c) 2005 The Gale Group
File   6:NTIS 1964-2005/Aug W3
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Aug W3
         (c) 2005 INIST/CNRS
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Aug W4
         (c) 2005 Inst for Sci Info
File  62:SPIN(R) 1975-2005/Jun W4
         (c) 2005 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jul
         (c) 2005 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2005/Jul W4
         (c) 2005 FIZ TECHNIK
```

17/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

08506345 E.I. No: EIP01035572630
Title: Research on a new type integrated security system
Author: Meng, Yang; Liu, Kelong; Qing, Sihan
Corporate Source: Inst of Software, Chinese Acad of Sciences, Beijing, China
Source: Ruan Jian Xue Bao/Journal of Software v 11 n 5 May 2000. p 616-619
Publication Year: 2000
CODEN: RUXUEW ISSN: 1000-9825
Language: Chinese
Document Type: JA; (Journal Article) Treatment: T; (Theoretical); G; (General Review)
Journal Announcement: 0104W4
Abstract: In this paper, a new Yaksha security system is presented based on ELGAMAL (NOT RSA) algorithm, The system is capable of **reusing** a single security infrastructure to perform various security functions-cryptography, digital signatures, distributed **authentication** and **key** exchange. At the same **time** , how the system can be used for **key** escrow is also described, one of the discussions which attract public attention. (Edited author abstract) 8 Refs.
Descriptors: *Security systems; Algorithms; Cryptography; Electronic document identification systems
Identifiers: Discrete logarithms; Distributed **authentication** ; **Key** escrow; Certification authorities; Integrated security systems; Yaksha security systems; Security infrastructure; Digital signatures; **Key** exchange; Elgamal algorithm
Classification Codes:
914.1 (Accidents & Accident Prevention); 911.2 (Industrial Economics); 901.3 (Engineering Research)
914 (Safety Engineering); 723 (Computer Software); 921 (Applied Mathematics); 911 (Industrial Economics); 901 (Engineering Profession)
91 (ENGINEERING MANAGEMENT); 72 (COMPUTERS & DATA PROCESSING); 92 (ENGINEERING MATHEMATICS); 90 (GENERAL ENGINEERING)

17/5/5 (Item 2 from file: 35)
DIALOG(R)File 35:Dissertation Abs Online

01681976 ORDER NO: AAD99-15127
AUTOMATED ACCESS CONTROL TO INCREASE OBJECT-ORIENTED COMPONENT REUSE
Author: MOEDJIONO, SARDJOENI
Degree: D.SC.
Year: 1999
Corporate Source/Institution: THE GEORGE WASHINGTON UNIVERSITY (0075)
Director: SHMUEL ROTENSTREICH
Source: VOLUME 59/12-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 6382. 111 PAGES
Descriptors: COMPUTER SCIENCE
Descriptor Codes: 0984

Software construction is increasingly complicated. Success will require breakthroughs in the production process and in methods and tools to assess and improve products. A technology for improving software quality and productivity is software **reuse** . To achieve an effective and efficient software construction requires software **reuse** facilities, promotions, and practices. Concepts, models, and support tools or frameworks for controlling, supporting, and easing the object-oriented system's design practices, development, operations, and maintenance are needed. Research must be wedded to large scale development. Some previous research results in software **reuse** technology support this need, i.e., to build the required model.

This dissertation research is focusing primarily on solving one of the technical problems in applying software **reuse** , i.e., the customization and/or composition problems. It introduces a required model, i.e., an Automated Access Control Model. This model contains a framework architecture of the access control mechanism as the core model and five other supporting concepts. The five supporting concepts are view's concept as a triple relation between server-client-operations, separation of objects into interface and implementation class lattices concept to represent the abstraction and encapsulation, **user** access connection concept to **authenticate** the **user** to use and access the system, and perform the authorized operations, object linking and embedding concept to be able to link or embed object(s) to applications, and automation concept to automate the applications to be able to expose operations/behaviors to the controller/client or to control the applications/servers by invoking/using the server's operations/behaviors.

The prototype of the model introduced above, combined with the other related models has been exercised in practical implementation to achieve the main objective of the object-oriented software construction, i.e., to promote or to increase the object-oriented component **reuse** .

The benefit of this model is to ease the object-oriented system developer's work, in designing, developing, operating, and maintaining their systems. It does this by automating the access control to objects, which in turn will greatly improve the software reusability by saving development and maintenance **time** and cost, increase the system's operation efficiency, and improve the system's productivity and quality.

17/5/12 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

7157390 INSPEC Abstract Number: B2002-02-6150M-065, C2002-02-5640-056
Title: Research and realization of HTTP authentication
Author(s): Ye Xi-jun; Wu Guo-xin; Xu Yong; Shu Kun
Author Affiliation: Comput. Center, Nanjing Agric. Univ., China
Journal: Computer Integrated Manufacturing Systems vol.7, no.3 p. 49-52
Publisher: Editorial Department of CIMS,
Publication Date: March 2001 Country of Publication: China
CODEN: JJZXFN ISSN: 1006-5911
SICI: 1006-5911(200103)7:3L.49:RRHA;1-#
Material Identity Number: H893-2001-003
Language: Chinese Document Type: Journal Paper (JP)
Treatment: Applications (A); Practical (P)
Abstract: HTTP is a kind of **stateless** protocol. Though HTTP provides basic **authentication** services to support the legal access of **users** , its function is weak. This paper introduces the digest access **authentication** technology that HTTP provides, analyzes the weakness of the frequently used "One **Time Password** " **authentication** method, and presents improvements and an implementation in Java. (6 Refs)
Subfile: B C
Descriptors: hypermedia; message **authentication** ; security of data; transport protocols
Identifiers: HTTP **authentication** ; legal access; digest access **authentication** technology; Java
Class Codes: B6150M (Protocols); C5640 (Protocols); C6130S (Data security)

17/5/17 (Item 9 from file: 2)
DIALOG(R)File 2:INSPEC

6314249 INSPEC Abstract Number: B1999-09-6120D-017, C1999-09-1260C-015
Title: Secure password **-based protocol for downloading a private** key
Author(s): Perlman, R.; Kaufman, C.
Author Affiliation: Sun Microsyst. Labs., Chelmsford, MA, USA
Conference Title: Proceedings 1999 Network and Distributed System Security Symposium p.3-11
Publisher: Internet Soc, Reston, VA, USA
Publication Date: 1999 Country of Publication: USA x+171 pp.
ISBN: 1 891562 04 5 Material Identity Number: XX-1999-00579
Conference Title: Proceedings of The Internet Society 1999 Network and Distributed System Security Symposium
Conference Sponsor: Internet Soc
Conference Date: 3-5 Feb. 1999 Conference Location: San Diego, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: We present protocols that allow a **user** Alice, knowing only her name and **password** , and not carrying a smart card, to " **log in** to the network" from a "generic" workstation, i.e., one that has all the necessary software installed, but none of the configuration information usually assumed to be known a priori in a security scheme, such as Alice's public and private **keys** , her certificate, and the public **keys** of one or more CAs. By "logging in", we mean the workstation retrieves this information on behalf of the **user** . This would be straightforward if Alice had a cryptographically strong **password** . We propose protocols that are secure even if Alice's **password** is guessable. We concentrate on the initial retrieval of Alice's private **key** from some server Bob on the network. We discuss various protocols for doing this that avoid off-line **password** guessing attacks by someone eavesdropping or impersonating Alice or Bob. We discuss auditable vs. unauditable on-line attacks, and present protocols that allow Bob to be **stateless** , avoid denial-of-service attacks, allow for salt, and are minimal in computation and number of messages. (11 Refs)
Subfile: B C
Descriptors: cryptography; protocols
Identifiers: **password** -based protocol; private **key** ; protocols; security scheme; denial-of-service attacks
Class Codes: B6120D (Cryptography); B6150M (Protocols); C1260C (Cryptography theory); C6130S (Data security); C5640 (Protocols)

17/5/20 (Item 12 from file: 2)
DIALOG(R)File 2:INSPEC

5201917
Title: Password **protection for NetWare [** Password **Sentry 1.0]**
Author(s): Chang, H.
Journal: PC User no.276 p.63
Publisher: EMAP Computing,
Publication Date: 7-20 Feb. 1996 Country of Publication: UK
CODEN: PCUSDW ISSN: 0263-5720
SICI: 0263-5720(19960207/20)276L.63:PPNP;1-J
Material Identity Number: E768-96002
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P); Product Review (R)
Abstract: **Password** Sentry 1.0 from BindView was developed to give NetWare servers an extra level of **password** authorisation to give a higher degree of **password** security than is provided within the existing product. NetWare`s existing **password** protection features ensure **passwords** cannot be the same as **login IDs** , specify minimum **password** length, make sure **passwords** are changed regularly and are not **reused** , and give intrusion protection. But these facilities do not stop **users** from choosing **passwords** that are easy to guess, such as their middle name. **Password** Sentry checks **password** security either when a **password** is changed or during a regular scan. It uses a built-in database of more than 1 million words, broken down into around 18 tables including legal, medical, computer and Star Trek terms and eight different languages. (0 Refs)
Subfile: D
Descriptors: authorisation; network operating systems; protection
Identifiers: **Password** Sentry 1.0; BindView; NetWare servers; **password** authorisation; **password** security; **password** protection; regular scan; **password** changes; built-in database
Class Codes: D1060 (Security); D5020 (Computer networks and intercomputer communications)

17/5/23 (Item 15 from file: 2)
DIALOG(R)File 2:INSPEC

03987198 INSPEC Abstract Number: C91064816
Title: Roles **for** users **and privileges for system processes: high-trust mechanisms for low-trust systems**
Author(s): Gill, D.L.
Conference Title: USENIX Workshop Proceedings. UNIX Security II p.61
Publisher: USENIX Assoc, Berkeley, CA, USA
Publication Date: 1990 Country of Publication: USA 173 pp.
Conference Date: 27-28 Aug. 1990 Conference Location: Portland, OR, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Summary form only given, as follows. To provide more trust for systems being developed to meet the C2 Class of Trusted Computer Systems Evaluation Criteria (TCSEC), a technique is suggested for systems providing audit; identification and **authentication** , and discretionary access control of and secure **reuse** of objects. The technique is to 'borrow' concepts from the B and A division of the TCSEC for use at the C division. The Defense Intelligence Agency (DIA) has developed a set of requirements known as the Compartmented Mode Workstation (CMW) requirements. These requirements take as a basis the Labeled Security Protection (B1) Class of the Department of Defense TCSEC and augment it with accountability and assurance requirements from the B2, B3 and even A1 classes of the TCSEC. The article discusses the TCSEC requirements used for defining the ones listed. It gives rational for consideration of such requirements in a C2 system, and discusses alternatives for implementation of the requirements listed. (0 Refs)
Subfile: C
Descriptors: security of data; Unix
Identifiers: secure **reuse** ; system processes; high-trust mechanisms; low-trust systems; C2 Class of Trusted Computer Systems Evaluation Criteria ; audit; identification; **authentication** ; discretionary access control; Defense Intelligence Agency; accountability; assurance requirements
Class Codes: C6150J (Operating systems); C6130 (Data handling techniques)

17/5/26 (Item 3 from file: 94)
DIALOG(R)File 94:JICST-EPlus

04287193 JICST ACCESSION NUMBER: 99A0772356 FILE SEGMENT: JICST-E
Reusable Secret Sharing Schemes.
KATAYANAGI KIYOKO (1); MURAKAMI YASUYUKI (1); KASAHARA MASAO (1); SAKAI RYUICHI (2)
(1) Kyoto Inst. of Technol., Fac. of Eng. and Des.; (2) Osaka Electro-Communication Univ.
Denshi Joho Tsushin Gakkai Gijutsu Kenkyu Hokoku(IEIC Technical Report (Institute of Electronics, Information and Communication Enginners), 1999, VOL.99,NO.208(ISEC99 11-25), PAGE.9-14, FIG.2, REF.4
JOURNAL NUMBER: S0532BBG
UNIVERSAL DECIMAL CLASSIFICATION: 621.391.037.3
LANGUAGE: Japanese COUNTRY OF PUBLICATION: Japan
DOCUMENT TYPE: Journal
ARTICLE TYPE: Original paper
MEDIA TYPE: Printed Publication
ABSTRACT: Secret Sharing Schemes make it possible to share a secret within a group, each **member** of which is given a different piece called share. It is possible to recover the secret if the certain number of **members** agree to do it. However once they recover the secret, all of them are notified the secret. Thus the shares cannot be **reused** . In this report, we propose Reusable Secret Sharing Schemes which are able to **authenticate** the secret, without renewing the shares, in many **times** . (author abst.)
DESCRIPTORS: **authentication** ; data protection; threshold; **reuse** ; cryptogram; matrix(mathematics); public **key** cryptography
IDENTIFIERS: secret **key** cryptosystem; ZKIP
BROADER DESCRIPTORS: protection; numerical value; utilization; algebraic system
CLASSIFICATION CODE(S): ND02030R

```
Set     Items   Description
S1          3   STATELESS(N)AUTHENTICATION(10N)(KEY OR KEYS)
File 349:PCT FULLTEXT 1979-2005/UB=20050901,UT=20050825
         (c) 2005 WIPO/Univentio
File 654:US Pat.Full. 1976-2005/Sep 01
         (c) Format only 2005 Dialog
```

1/3,K/3 (Item 2 from file: 654)
DIALOG(R)File 654:US Pat.Full.

0004935153 **IMAGE Available
Derwent Accession: 2002-216558
Authentication method and schemes for data integrity protection
Inventor: Virgil Gligor, INV
Pompiliu Donescu, INV
Correspondence Address: William T. Ellis FOLEY & LARDNER, Washington Harbour 3000 K Street, N.W., Suite 500, Washington, DC, 20007-5109, US

	Publication Number	Kind	Date	Application Number	Filing Date
Main Patent	US 20010046292	A1	20011129	US 2001818608	20010328
Provisional				US 60-193447	20000331

Fulltext Word Count: 32836

Description of the Invention:
...FIG. 9 illustrates a schematic diagram for an alternate embodiment of this invention of the **stateless authentication** scheme using a single secret **key** K 31 shared by the sender and receiver. The input string x 23 (which is...

...of blocks of the input plaintext string. For instance, for the preferred embodiment of the **stateless authentication** scheme using two secret **keys** K and K' (viz., FIG. 5), if r[sub]o, the random number of the...

...message signing procedure applies to all other embodiments of this invention, not just to the **stateless authentication** scheme using two secret **keys** K and K...

...out-of-order processing of tag verification. For instance, for the preferred embodiment of the **stateless authentication** scheme using two secret **keys** K and K' (viz., FIG. 6), if the random number r[sub]o is received...

...of tag verification applies to all other embodiments of this invention, not just to the **stateless authentication** scheme using two secret **keys** K and K' (described in FIGS. 5 and 6...

```
Set     Items   Description
S1      54663   AUTHENTICAT? OR LOGIN OR LOGON OR SIGNIN OR SIGNON OR (LOG
             OR SIGN)()("IN" OR ON) OR PASSWORD? OR PASS()(WORD OR WORDS OR
              PHRASE?)
S2     160041   GLOBAL UNIVERSAL OR "NOT"()STATEFUL OR STATELESS OR REUSE?
              OR RECYCLE? OR USE()AGAIN? OR RE()(USE OR CYCLE OR USING) OR
             REUSING OR RECYCLING OR STATE()LESS OR SESSIONLESS
S3     409552   KEY OR KEYS OR IDENTIFIER? OR BIT()STRING? ? OR ID OR IDS -
             OR LABEL OR LABELS
S4    2216079   SECURITY()CONTEXT? OR ORGANIZATION? OR USER? OR INDIVIDUAL?
              OR MEMBER? OR EMPLOYEE?
S5    5755856   LOCATION? OR ROLE? OR ACCESS()LEVEL? OR EXPIRATION? OR POS-
             ITION? OR TIME OR DATE OR TIMES OR DATES OR DURATION
S6         54   S1 AND S2 AND S3
S7         38   S6 AND (S4 OR S5)
S8         25   S7 NOT AD=20010419:20030419
S9         21   S8 NOT AD=20030419:20050905
S10        17   S9 AND IC=(G06F OR H04L)
S11        30   S6 AND (KEY OR KEYHANDLE? OR KEYS)
S12        13   S11 NOT S8
S13        26   S1 AND S2 AND S4 AND S5
S14        22   S13 AND IC=(G06F OR H04L OR H04N)
S15        34   S12 OR S14
S16        21   S15 NOT S7
S17        11   S16 NOT AD=20010419:20040419
S18        11   S17 NOT AD=20040419:20050922
S19      2425   (ONE OR SINGLE OR ONLY OR CENTRAL? OR UNIVERSAL? OR GLOBAL?
              OR SYSTEM()WIDE)(2N)S1
S20    126450   (MULTIPL? OR PLURAL OR MANY OR SEVERAL OR DIFFERENT OR VAR-
             IOUS OR VARIET? OR DISTRIBUTED)(2N)(SYSTEM? OR MODULE? OR PRO-
             GRAM? OR NODE? ? OR WORKSTATION? OR WORK()STATION?)
S21        98   S19 AND S20
S22        10   S21 AND (KEY OR KEYHANDLE? OR KEYS OR KEYPAIR?)
S23         2   S21 AND (ALGORITHM? OR FORMULA? OR CALCULATION?)
S24        12   S22 OR S23
S25        10   S22 NOT (S18 OR S7 OR S12)
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200555
        (c) 2005  Thomson Derwent
```

25/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

06753409 **Image available**
PASSWORD INTEGRATION MANAGEMENT SYSTEM

PUB. NO.: 2000-339271 [JP 2000339271 A]
PUBLISHED: December 08, 2000 (20001208)
INVENTOR(s): MIHASHI TOSHIYUKI
APPLICANT(s): NEC CORP
APPL. NO.: 11-150649 [JP 99150649]
FILED: May 28, 1999 (19990528)
INTL CLASS: G06F-015/00; G06F-013/00

ABSTRACT

PROBLEM TO BE SOLVED: To provide a password integration management system which efficiently manages an access to a distribution connected processor.

SOLUTION: An ID number and a password are inputted from an input device 2 connected to a terminal 1 for displaying a job screen. A job server 3 has an ID storage part 31 for storing the ID number and a cryptographic **key** encoding part 32 for decoding the cryptographic **key** , and executes job processing. An authentication server 4 has an ID/password storage part 41 for storing association between the ID number and the password and a cryptographic **key** generation part 42 for generating the cryptographic **key** , and stores authentication information. In this structure, it is integrally managed whether or not it is valid to start job processing in a distribution connected processor. Thus, in jog start processing in **plural** job **system** , job start of all system is enabled by a **single** user ID/ **password** without a system user being conscious of all the user ID/password managed by individual system and using them for different purposes.

25/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

05249196 **Image available**
AUTHENTICATION METHOD IN COMMUNICATION **SYSTEM** HAVING **PLURAL** EQUIPMENTS

PUB. NO.: 08-204696 [JP 8204696 A]
PUBLISHED: August 09, 1996 (19960809)
INVENTOR(s): MANUERU SERESEDO
IWAMURA KEIICHI
APPLICANT(s): CANON INC [000100] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 07-008184 [JP 958184]
FILED: January 23, 1995 (19950123)
INTL CLASS: [6] H04L-009/00; H04L-009/10; H04L-009/12; G06F-015/00; G09C-001/00; H04L-029/06
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 44.9 (COMMUNICATION -- Other); 45.4 (INFORMATION PROCESSING -- Computer Applications)

ABSTRACT

PURPOSE: To provide a distributed authentication server having the same authentication function as that of a **centralized** management type **authentication** server and realizing high fault tolerance.

CONSTITUTION: In the communication system including a device 14 being a distributed authentication server, a authentication receiver 15 requesting authentication sends a authentication request message including identifier of a authentication receiver and that of a authentication server to each device 14 of the distributed authentication server and each device 14 of the distributed authentication server generates a ciphered authentication identifier by a secret **key** relating to the authentication receiver based on the authentication request message in the common. Then the authentication message is generated by ciphering the authentication identifier with a secret **key** relating to the authentication receiver and each device 14 of the distributed authentication server sends the authentication message to the authentication receiver 15. Then the authentication receiver 15 receiving the authentication message decodes the authentication message and sends the obtained authentication identifier to the authentication server 15, and the authentication server 15 receiving the authentication identifier decodes the authentication identifier to verify the authentication receiver.

```
Set     Items   Description
S1      54663   AUTHENTICAT? OR LOGIN OR LOGON OR SIGNIN OR SIGNON OR (LOG
             OR SIGN)()("IN" OR ON) OR PASSWORD? OR PASS()(WORD OR WORDS OR
              PHRASE?)
S2     160041   GLOBAL UNIVERSAL OR "NOT"()STATEFUL OR STATELESS OR REUSE?
              OR RECYCLE? OR USE()AGAIN? OR RE()(USE OR CYCLE OR USING) OR
             REUSING OR RECYCLING OR STATE()LESS OR SESSIONLESS
S3     409552   KEY OR KEYS OR IDENTIFIER? OR BIT()STRING? ? OR ID OR IDS -
             OR LABEL OR LABELS
S4    2216079   SECURITY()CONTEXT? OR ORGANIZATION? OR USER? OR INDIVIDUAL?
              OR MEMBER? OR EMPLOYEE?
S5    5755856   LOCATION? OR ROLE? OR ACCESS()LEVEL? OR EXPIRATION? OR POS-
             ITION? OR TIME OR DATE OR TIMES OR DATES OR DURATION
S6         54   S1 AND S2 AND S3
S7         38   S6 AND (S4 OR S5)
S8         25   S7 NOT AD=20010419:20030419
S9         21   S8 NOT AD=20030419:20050905
S10        17   S9 AND IC=(G06F OR H04L)
S11        30   S6 AND (KEY OR KEYHANDLE? OR KEYS)
S12        13   S11 NOT S8
S13        26   S1 AND S2 AND S4 AND S5
S14        22   S13 AND IC=(G06F OR H04L OR H04N)
S15        34   S12 OR S14
S16        21   S15 NOT S7
S17        11   S16 NOT AD=20010419:20040419
S18        11   S17 NOT AD=20040419:20050922
S19      2425   (ONE OR SINGLE OR ONLY OR CENTRAL? OR UNIVERSAL? OR GLOBAL?
              OR SYSTEM()WIDE)(2N)S1
S20    126450   (MULTIPL? OR PLURAL OR MANY OR SEVERAL OR DIFFERENT OR VAR-
             IOUS OR VARIET? OR DISTRIBUTED)(2N)(SYSTEM? OR MODULE? OR PRO-
             GRAM? OR NODE? ? OR WORKSTATION? OR WORK()STATION?)
S21        98   S19 AND S20
S22        10   S21 AND (KEY OR KEYHANDLE? OR KEYS OR KEYPAIR?)
S23         2   S21 AND (ALGORITHM? OR FORMULA? OR CALCULATION?)
S24        12   S22 OR S23
S25        10   S22 NOT (S18 OR S7 OR S12)
S26         3   S21 AND S2
S27         3   S26 NOT S25
File 347:JAPIO Nov 1976-2005/Apr(Updated 050801)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200555
        (c) 2005  Thomson Derwent
```

27/5/2 (Item 2 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015332137 **Image available**
WPI Acc No: 2003-393072/200337
XRPX Acc No: N03-314171

Access management method in distributed **data processing** system , **involves sending response accompanied by aggregator token having uniform resource identifier after successful completion of client authentication process**

Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: FLURRY G A; LAWTON B; NICKOLAS S E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 20030061512	A1	20030327	US 2001965736	A	20010927	200337	B

Priority Applications (No Type Date): US 2001965736 A 20010927
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20030061512	A1		21	H04L-009/32	

Abstract (Basic): US 20030061512 A1

NOVELTY - A request to access resource protected by an application service provider (ASP) aggregator service that provides **single - sign - on** functionality for non-sourced applications hosted by ASP is received from a client. The client is required to successfully complete an authentication process after which a response accompanied by an aggregator token comprising uniform resource identifier is sent to the client.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(1) apparatus for access management in a **distributed** data processing **system** ; and

(2) computer program product in a computer readable medium for performing the method of access management.

USE - For access management in **distributed** data processing **system** .

. ADVANTAGE - A coherent interface is maintained between the user and the ASP architecture. The user attempts to **reuse** saved session information directly with a hosted application is recovered due to the **single - sign - on** mechanism within an ASP infrastructure. The modification to an ASP aggregator services infrastructure is minimum. The infrastructure of ASP aggregator service is easily modified.

DESCRIPTION OF DRAWING(S) - The figure shows a temporal flow diagram that depicts some of the action and communication traffic for a **single - sign - on** operation with an ASP aggregator service.

pp; 21 DwgNo 4/5

Title Terms: ACCESS; MANAGEMENT; METHOD; DISTRIBUTE; DATA; PROCESS; SYSTEM; SEND; RESPOND; ACCOMPANIED; TOKEN; UNIFORM; RESOURCE; IDENTIFY; AFTER; SUCCESS; COMPLETE; CLIENT; AUTHENTICITY; PROCESS
Derwent Class: T01
International Patent Class (Main): H04L-009/32
File Segment: EPI